I2NSF Consumer-Facing Interface YANG Data Model

(draft-jeong-i2nsf-consumer-facing-interface-dm-03)

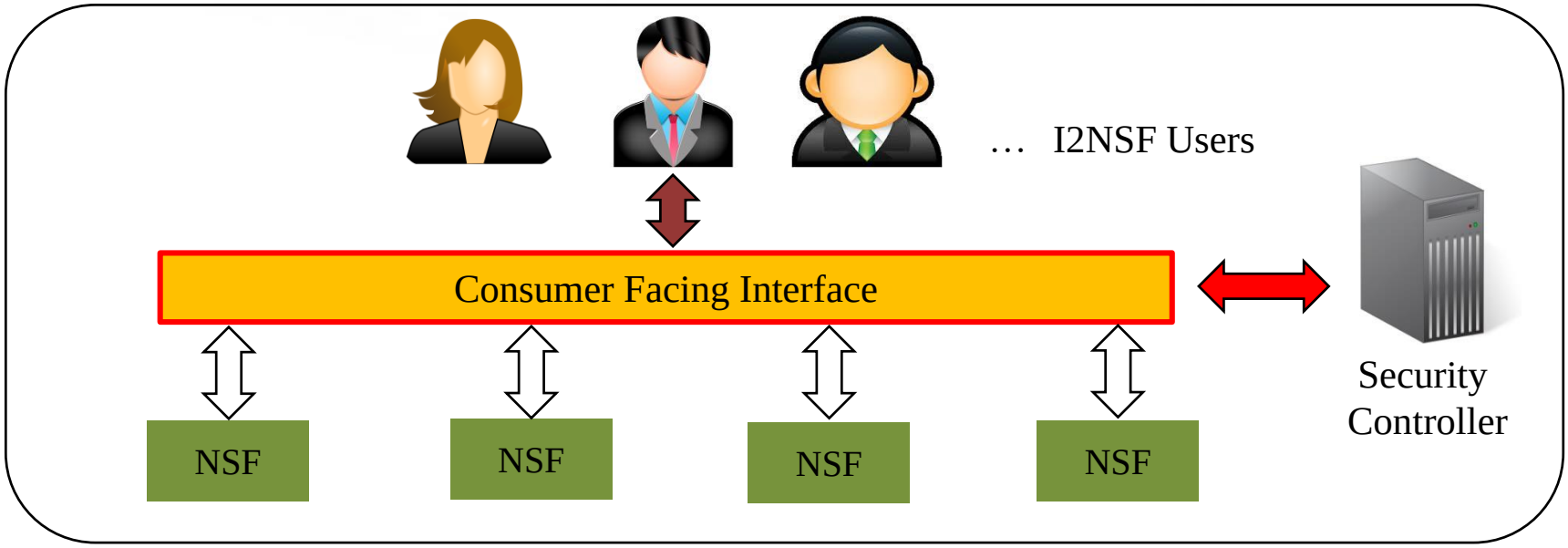
IETF 99, Prague, Czech

July 18, 2017

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

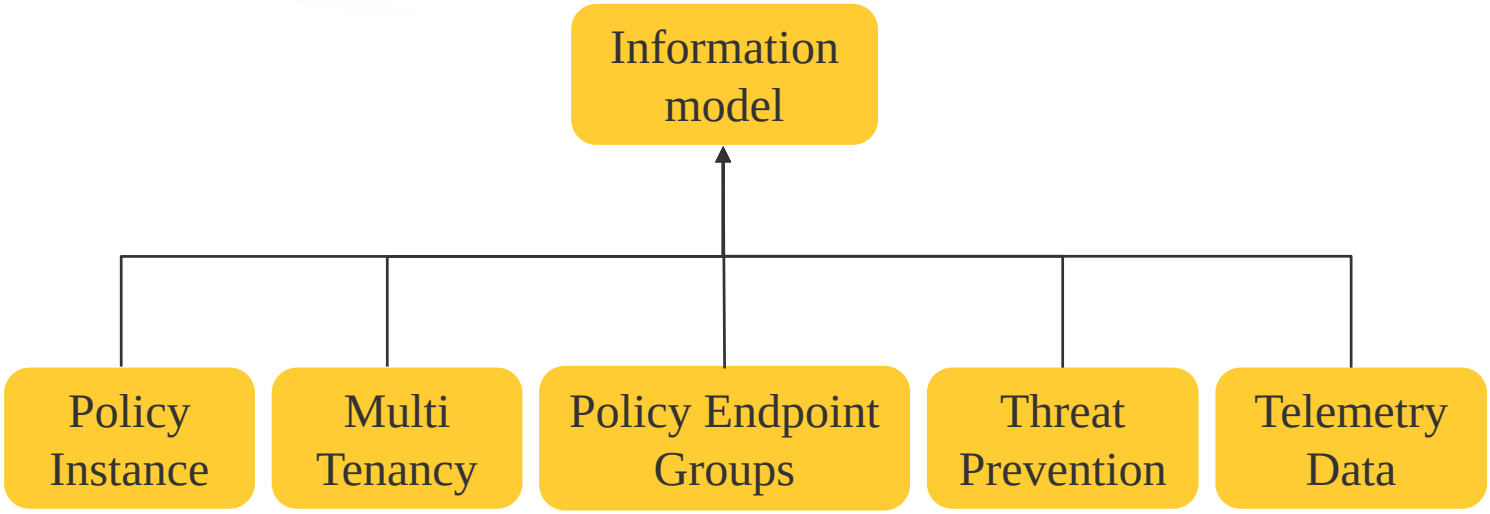
Introduction

- This document describes a YANG data model for Consumer-Facing Interface in an I2NSF system in an NFV environment.
- A data model is required for enabling different users of an I2NSF system to manage security policies.



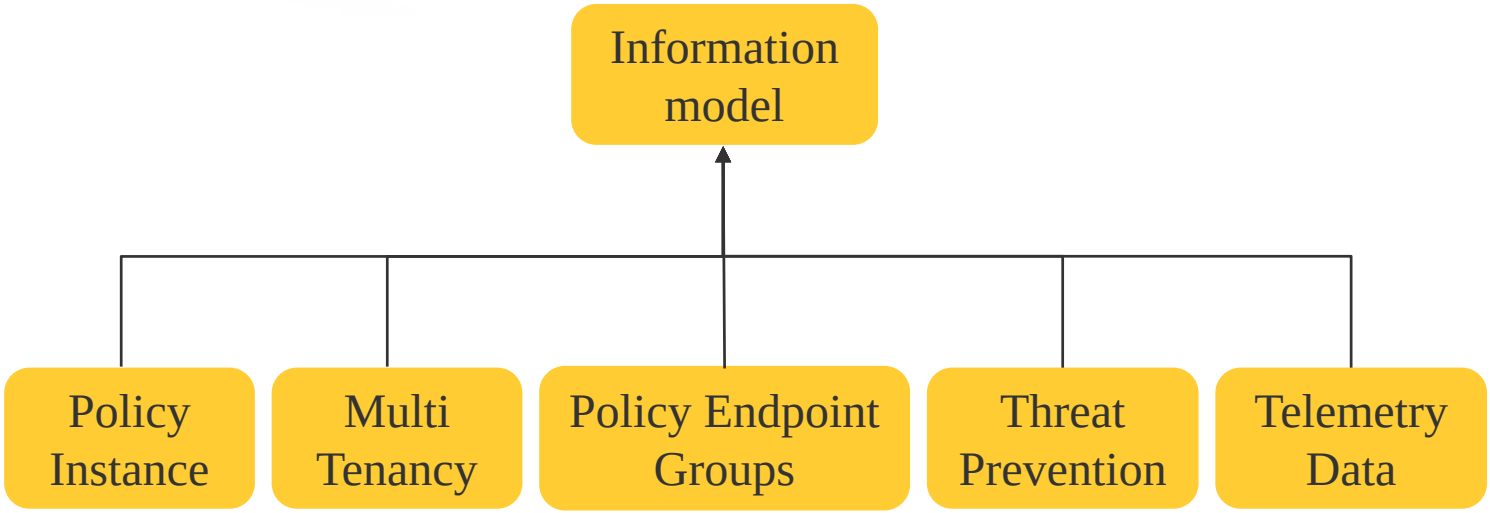
Introduction

- The data model is derived from the information model in draft-kumar-i2nsf-client-facing-interface-im-02
- The information model describes the managed objects with each object capturing a unique set of information from security admin need to express a security policy, and relationship among them.



Introduction

- The main objective of this data model is to fully transform the information model into a YANG data model that can be used for delivering control via the Consumer-Facing Interface



Update from -01 and -02 Versions

- The following changes are made from draft-jeong-i2nsf-consumer-facing-interface-dm-01 and -02.
  - The overall architecture diagram of security management system has been removed.
  - Data tree model has been revised according to draft-kumar-i2nsf-client-facing-interface-im-02.
  - YANG data model has been revised using the data tree model.
  - Two YANG compilation warnings are resolved.

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]
```

Policy Endpoint Groups

```
+--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 Prevention

```
+--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 Instance

```
+--rw policy-instance
   +--rw policy-calendar* [policy-calendar-id]
      +--rw policy-calendar-id              uint16
      +--rw name?                           string
      +--rw date?                           yang:date-and-time
      +--rw enforcement-type?               enumeration
      +--rw time-information?               string
      +--rw event-map?                      string
   +--rw policy-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 policy-rule* [policy-rule-id]
      +--rw policy-rule-id                  string
      +--rw name?                           string
      +--rw date?                           yang:date-and-time
      +--rw source?                         string
      +--rw destination?                    string
      +--rw exception?                      string
      +--rw action?                         string
      +--rw precedence?                     uint8
   +--rw policy-instance* [policy-instance-id]
      +--rw policy-instance-id              string
      +--rw name?                           string
      +--rw date?                           yang:date-and-time
      +--rw rules?                          string
      +--rw scheduling-type?                enumeration
      +--rw scheduling-information?         string
      +--rw owner?                          string
```

Data Model for Consumer-Facing Interface

```
+--rw policy-instance
   +--rw policy-calendar* [policy-calendar-id]
   |  +--rw policy-calendar-id              uint16
   |  +--rw name?                           string
   |  +--rw date?                           yang:date-and-time
   |  +--rw enforcement-type?               enumeration
   |  +--rw time-information?               string
   |  +--rw event-map?                      string
   +--rw policy-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 policy-rule* [policy-rule-id]
   |  +--rw policy-rule-id                  string
   |  +--rw name?                           string
   |  +--rw date?                           yang:date-and-time
   |  +--rw source?                         string
   |  +--rw destination?                    string
   |  +--rw exception?                      string
   |  +--rw action?                         string
   |  +--rw precedence?                     uint8
   +--rw policy-instance* [policy-instance-id]
      +--rw policy-instance-id              string
      +--rw name?                           string
      +--rw date?                           yang:date-and-time
      +--rw rules?                          string
      +--rw scheduling-type?                enumeration
      +--rw scheduling-information?         string
      +--rw owner?                          string
```

The data model consists of:

- **Multi Tenancy**
- **Policy Endpoint Groups**
- **Threat Prevention**
- **Telemetry Data**
- **Policy Instance**

The Policy Instance of data model consists of:

- **Policy Calendar**
- **Policy Action**
- **Policy Rule**
- **Policy Instance**

Data Model for Consumer-Facing Interface

```
+--rw policy-instance
   +--rw policy-calendar* [policy-calendar-id]
   |  +--rw policy-calendar-id                uint16
   |  +--rw name?                             string
   |  +--rw date?                             yang:date-and-time
   |  +--rw enforcement-type?                 enumeration
   |  +--rw time-information?                 string
   |  +--rw event-map?                        string
   +--rw policy-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 policy-rule* [policy-rule-id]
   |  +--rw policy-rule-id                    string
   |  +--rw name?                             string
   |  +--rw date?                             yang:date-and-time
   |  +--rw source?                           string
   |  +--rw destination?                      string
   |  +--rw exception?                        string
   |  +--rw action?                           string
   |  +--rw precedence?                       uint8
   +--rw policy-instance* [policy-instance-id]
      +--rw policy-instance-id                string
      +--rw name?                             string
      +--rw date?                             yang:date-and-time
      +--rw rules?                            string
      +--rw scheduling-type?                  enumeration
      +--rw scheduling-information?           string
      +--rw owner?                            string
```

Policy rule
Represents the specific information about a high-level policy based on ECA (event-condition-action).

Event
Determines the 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, or establishing secure tunnels.

Policy Instance for VoIP/VoLTE Security Services

```
module ietf-i2nsf-consumer-facing-interface-policy-instance
 +--rw policy-instance
    +--rw policy-rule* [policy-rule-id]
    |  +--rw policy-rule-id          uint16
    |  +--rw name?                   string
    |  +--rw date?                   yang:date-and-time
    |  +--rw source?                 string
    |  +--rw destination?            string
    |  +--rw exception?              boolean
    |  +--rw exception-detail?       string
    +--rw action* [action-id]
    |  +--rw action-id               string
    |  +--rw name?                   string
    |  +--rw date?                   yang:date-and-time
    |  +--rw primary-action?         string
    |  +--rw secondary-action?       string
    +--rw precedence* [precedence-id]
    |  +--rw precedence-id           string
    |  +--rw rule-exist?             boolean
    +--rw event* [event-id]
    |  +--rw event-id                string
    |  +--rw security-event?         string
    |  +--rw threat-map?             string
    |  +--rw enable?                 boolean
    +--rw condition* [condition-id]
    |  +--rw condition-id            string
    |  +--rw caller* [caller-id]
    |  |  +--rw caller-id            uint16
    |  |  +--rw caller-id-id?        string
    |  |  +--rw caller-country?      string
    |  |  +--rw caller-city?         string
    |  +--rw callee* [callee-id]
    |     +--rw callee-id            uint16
    |     +--rw callee-id-id?        string
    |     +--rw callee-country?      string
    |     +--rw callee-city?         string
    +--rw policy-calendar* [policy-calendar-id]
       +--rw policy-calendar-id      uint16
       +--rw name?                   string
       +--rw date?                   yang:date-and-time
       +--rw enforcement-type?       string
       +--rw begin-time?             yang:date-and-time
       +--rw end-time?               yang:date-and-time
```

Multi-tenancy, endpoint groups, threat prevention, and telemetry data components are general part of the tree model.

So we can just modify the policy instance in order to generate and enforce high-level policies.

Policy Instance for VoIP/VoLTE Security Services

```
module ietf-i2nsf-consumer-facing-interface-policy-instance
 +--rw policy-instance
    +--rw policy-rule* [policy-rule-id]
    |  +--rw policy-rule-id          uint16
    |  +--rw name?                   string
    |  +--rw date?                   yang:date-and-time
    |  +--rw source?                 string
    |  +--rw destination?            string
    |  +--rw exception?              boolean
    |  +--rw exception-detail?       string
    +--rw action* [action-id]
    |  +--rw action-id               string
    |  +--rw name?                   string
    |  +--rw date?                   yang:date-and-time
    |  +--rw primary-action?         string
    |  +--rw secondary-action?       string
    +--rw precedence* [precedence-id]
    |  +--rw precedence-id           string
    |  +--rw rule-exist?             boolean
    +--rw event* [event-id]
    |  +--rw event-id                string
    |  +--rw security-event?         string
    |  +--rw threat-map?             string
    |  +--rw enable?                 boolean
    +--rw condition* [condition-id]
    |  +--rw condition-id            string
    |  +--rw caller* [caller-id]
    |  |  +--rw caller-id            uint16
    |  |  +--rw caller-id-id?        string
    |  |  +--rw caller-country?      string
    |  |  +--rw caller-city?         string
    |  +--rw callee* [callee-id]
    |     +--rw callee-id            uint16
    |     +--rw callee-id-id?        string
    |     +--rw callee-country?      string
    |     +--rw callee-city?         string
    +--rw policy-calendar* [policy-calendar-id]
       +--rw policy-calendar-id      uint16
       +--rw name?                   string
       +--rw date?                   yang:date-and-time
       +--rw enforcement-type?       string
       +--rw begin-time?             yang:date-and-time
       +--rw end-time?               yang:date-and-time
```

Event, Condition, Action can be revised for the VoIP/VoLTE security services.

The policy-calendar can act as a scheduler to set the start and end time.

Next Step

- **Synchronization with SUPA's Information Model**
- **Reflection of the latest Consumer-Facing Interface's Information Model**
- **Implementation of More Use Cases in IETF-100 Hackathon**
  e.g., Deep packet inspection and DDoS-attack mitigation