Data Models of Interface to Network Security Functions (I2NSF)

IETF 102, Montreal

July 18, 2018

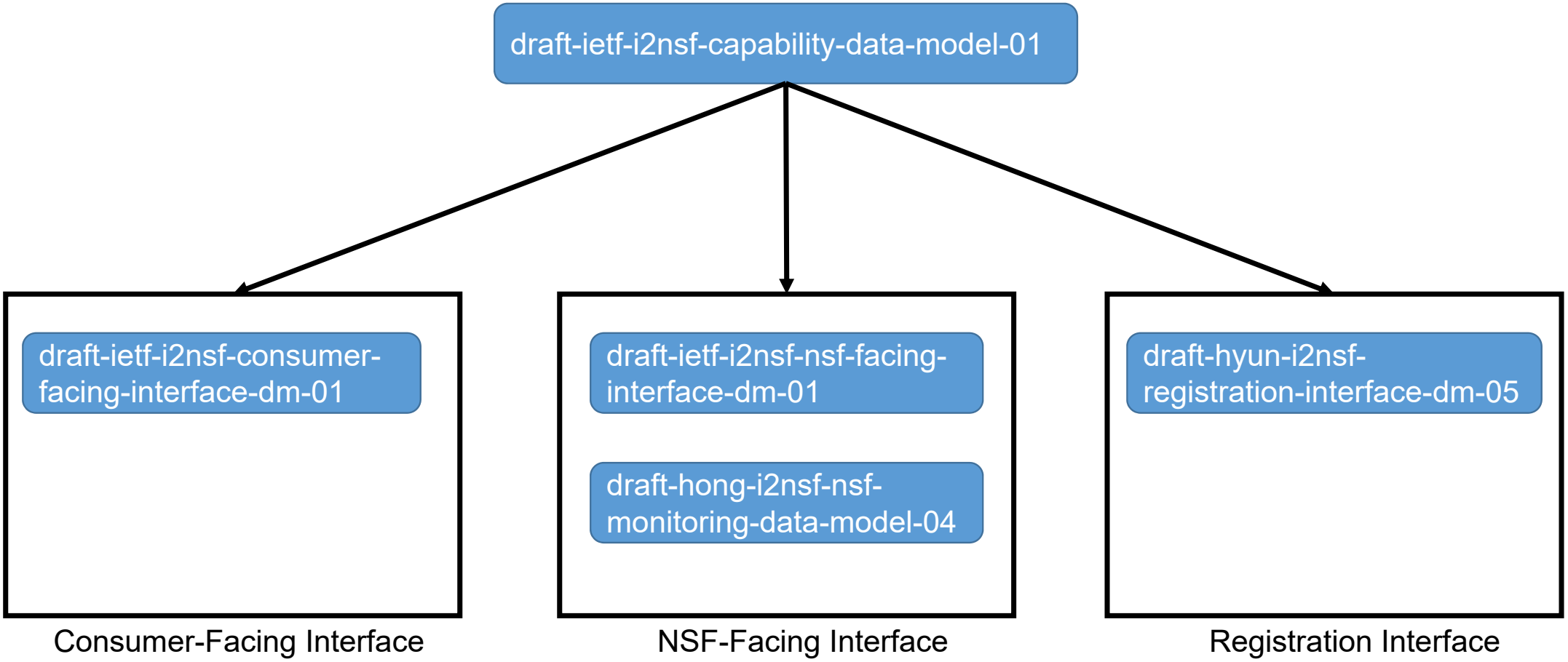
Jaehoon Paul Jeong

pauljeong@skku.edu

Data Models of I2NSF

- draft-ietf-i2nsf-capability-data-model-01
  - Capabilities of NSFs
- draft-ietf-i2nsf-consumer-facing-interface-dm-01
  - Consumer-Facing Interface
- draft-ietf-i2nsf-nsf-facing-interface-dm-01
  - NSF-Facing Interface
- draft-hyun-i2nsf-registration-interface-dm-05
  - Registration Interface
- draft-hong-i2nsf-nsf-monitoring-data-model-04
  - NSF-Facing Interface

Data Models of I2NSF



I2NSF Capability YANG Data Model
(draft-ietf-i2nsf-capability-data-model-01)

Susan Hares, Jaehoon Paul Jeong, Jinyong (Tim) Kim,

Robert Moskowitz, and Qiushi Lin

Updates from the Previous Version

- The Previous Draft:
  - draft-ietf-i2nsf-capability-data-model-00

- This draft defines a YANG Data Model (DM) corresponding to the Information Models (IMs) for NSF-Facing Interface and Registration Interface.
  - draft-ietf-i2nsf-capabilities-02
  - draft-hyun-i2nsf-registration-interface-im-06

- This data model is the base data model for other data models.
  - draft-ietf-i2nsf-consumer-facing-interface-dm-01
  - draft-ietf-i2nsf-nsf-facing-interface-dm-01
  - draft-hyun-i2nsf-registration-interface-dm-05
  - draft-hong-i2nsf-nsf-monitoring-data-model-04

- This YANG data module was verified through a prototype implemented at IETF-102 Hackathon.

List of Changes

- Consistency with capability information model
  - draft-ietf-i2nsf-capabilities-02
- Clarification and simplification of capabilities
- Addition of condition capabilities
- Replacement from unnecessary leaf-list to leaf
- Addition of NSF capabilities for content security and attack mitigation

Addition of condition capabilities

```
|  +--rw acl-number?                      boolean
|  +--rw application-condition
|  |  +--rw application-object?   boolean
|  |  +--rw application-group?    boolean
|  |  +--rw application-label?    boolean
|  |  +--rw category
|  |     +--rw application-category?   boolean
```

Application condition

```
+--rw url-category-condition
|  +--rw pre-defined-category?    boolean
|  +--rw user-defined-category?   boolean
```

URL category condition

Replacement from unnecessary leaf-list to leaf

OLD:

```
+--rw packet-security-udp-condition
|  +--rw pkt-sec-cond-udp-src-port?    boolean
|  +--rw pkt-sec-cond-udp-dest-port?   boolean
```

```
leaf-list pkt-sec-cond-udp-src-port {
  type boolean;
  description
    "This is a mandatory string attribute, and
    defines the UDP Source Port number (16 bits).";
}

leaf-list pkt-sec-cond-udp-dest-port {
  type boolean;
  description
    "This is a mandatory string attribute, and
    defines the UDP Destination Port number (16 bits).";
}
```

NEW:

```
+--rw packet-security-udp-condition
|  +--rw pkt-sec-cond-udp-src-port?    boolean
|  +--rw pkt-sec-cond-udp-dest-port?   boolean
```

```
leaf pkt-sec-cond-udp-src-port {
  type boolean;
  description
    "This is a mandatory string attribute, and
    defines the UDP Source Port number (16 bits).";
}

leaf pkt-sec-cond-udp-dest-port {
  type boolean;
  description
    "This is a mandatory string attribute, and
    defines the UDP Destination Port number (16 bits).";
}
```

Addition of NSF Capabilities for Content Security and Attack Mitigation

```
+--rw complete-nsf-capabilities
  +--rw con-sec-control-capabilities
  |  +--rw anti-virus?              boolean
  |  +--rw ips?                     boolean
  |  +--rw ids?                     boolean
  |  +--rw url-filter?              boolean
  |  +--rw data-filter?             boolean
  |  +--rw mail-filter?             boolean
  |  +--rw sql-filter?              boolean
  |  +--rw file-blocking?           boolean
  |  +--rw file-isolate?            boolean
  |  +--rw pkt-capture?             boolean
  |  +--rw application-behavior?    boolean
  |  +--rw voip-volte?              boolean
  +--rw attack-mitigation-capabilities
```

Content Security Capabilities

```
+--rw complete-nsf-capabilities
  ...
  +--rw attack-mitigation-capabilities
     +--rw (attack-mitigation-control-type)?
        +--:(ddos-attack)
        |  +--rw (ddos-attack-type)?
        |     +--:(network-layer-ddos-attack)
        |     |  +--rw network-layer-ddos-attack-types
        |     |     +--rw syn-flood-attack?           boolean
        |     |     +--rw udp-flood-attack?           boolean
        |     |     +--rw icmp-flood-attack?          boolean
        |     |     +--rw ip-fragment-flood-attack?   boolean
        |     |     +--rw ipv6-related-attack?        boolean
        |     +--:(app-layer-ddos-attack)
        |        +--rw app-layer-ddos-attack-types
        |           +--rw http-flood-attack?      boolean
        |           +--rw https-flood-attack?     boolean
        |           +--rw dns-flood-attack?       boolean
        |           +--rw dns-amp-flood-attack?   boolean
        |           +--rw ssl-flood-attack?       boolean
        +--:(single-packet-attack)
           +--rw (single-packet-attack-type)?
              +--:(scan-and-sniff-attack)
              |  +--rw ip-sweep-attack?           boolean
              |  +--rw port-scanning-attack?      boolean
              +--:(malformed-packet-attack)
              |  +--rw ping-of-death-attack?      boolean
              |  +--rw teardrop-attack?           boolean
              +--:(special-packet-attack)
                 +--rw oversized-icmp-attack?    boolean
                 +--rw tracert-attack?           boolean
```

Attack Mitigation Capabilities

Next Steps

- We will continue to work for the YANG data model of Object-Oriented (OO) Style.

- We will verify the YANG data model by implementing a prototype in the IETF Hackathon-103.
  - Registration Interface

I2NSF Data Model of Consumer-Facing Interface for Security Management (draft-ietf-i2nsf-consumer-facing-interface-dm-01)

Jaehoon (Paul) Jeong, Eunsoo Kim, Tae-Jin Ahn,

Rakesh Kumar, and Susan hares

Updates from the Previous Version

- The Previous Draft:
  - draft-ietf-i2nsf-consumer-facing-interface-dm-00

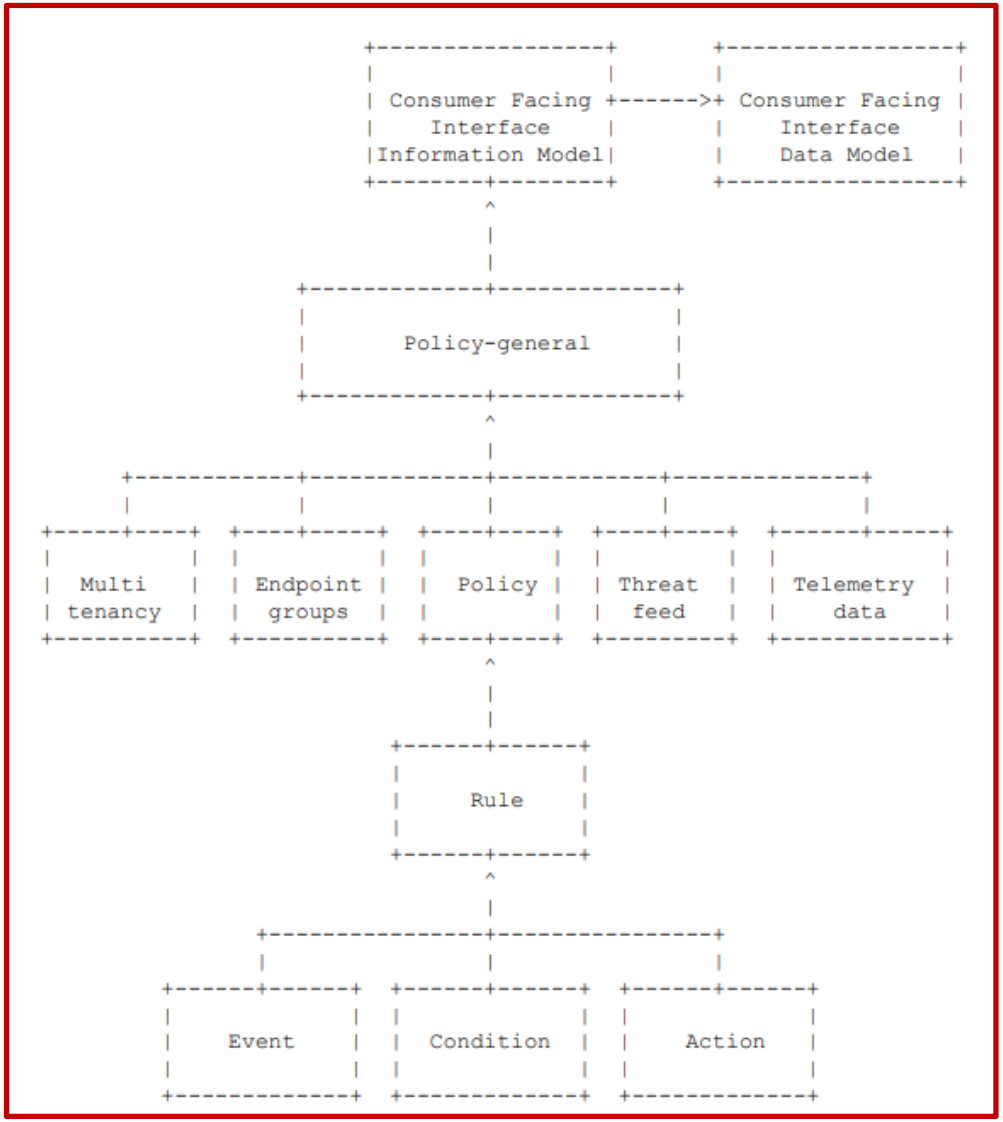
- This document defines a YANG Data Model (DM) corresponding to the Requirements and Information Model (IM) for Consumer-Facing Interface (CFI):
  - draft-ietf-i2nsf-client-facing-interface-req-05
  - draft-kumar-i2nsf-client-facing-interface-im-07

- This YANG data module was verified through a prototype implemented at IETF-102 Hackathon.

List of Updates

- The following changes are made from draft-ietf-i2nsf-consumer-facing-interface-dm-01
  - The diagram representing the high-level abstraction for consumer facing interface.
  - Minor changes in the name of objects for synchronizing to the information model.

Modification of YANG module



- A diagram representing the high-level abstraction for consumer facing interface (CFI).
- The diagram describes the objects consisting the CFI information model and the derivation of the data model.

Next Steps

- We will change the current YANG data model to the YANG data model of Object-Oriented (OO) Style.

- We will verify the YANG data model by implementing a prototype in the IETF Hackathon-103.
  - Consumer-Facing Interface

Network Security Functions Facing Interface YANG Data Model

(draft-ietf-i2nsf-nsf-facing-interface-dm-01)

Jinyong (Tim) Kim, Jaehoon Paul Jeong, Jung-Soo Park,

Susan Hares, and Qiushi Lin

Updates from the Previous Version

- The Previous Draft:
  - draft-ietf-i2nsf-nsf-facing-interface-dm-00

- This document defines a YANG Data Model (DM) corresponding to the Information Model (IM) for NSF-Facing Interface:
  - draft-ietf-i2nsf-capability-02

- This data model is derived from capability data model.
  - draft-ietf-i2nsf-capability-data-model-01

- This YANG data module was verified through a prototype implemented at IETF-102 Hackathon.

List of Updates

- Consistency with capability information model
  - draft-ietf-i2nsf-capabilities-02

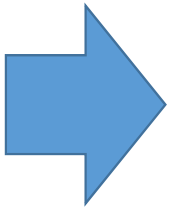
- Xia's Comments
  - Modification of YANG module
    - ✓ From a policy list to a policy container (Resolved)
    - ✓ From a rule id to a rule name (Resolved)
    - ✓ Default action (Resolved)
  - Addition of additional attributes for a policy
    - ✓ Session time (Resolved)
    - ✓ Rule group (Resolved)
    - ✓ Rule log (Resolved)
    - ✓ Additional conditions (Resolved)

Modification of YANG module

- From a policy list to a policy container

OLD:

```
module: ietf-i2nsf-policy-rule-for-nsf
+--rw i2nsf-security-policy* [policy-name]
|  +--rw policy-name?                string
|  +--rw eca-policy-rules* [rule-id]
|  |  +--rw rule-id                              uint8
|  |  +--rw rule-description?                      string
|  |  +--rw rule-priority?                         uint8
|  |  +--rw policy-event-clause-agg-ptr*           instance-identifier
|  |  +--rw policy-condition-clause-agg-ptr*       instance-identifier
|  |  +--rw policy-action-clause-agg-ptr*          instance-identifier
```



NEW:

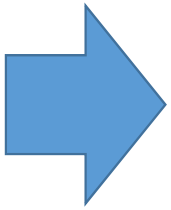
```
module: ietf-i2nsf-policy-rule-for-nsf
+--rw i2nsf-security-policy
|  +--rw policy-name?                string
|  +--rw rules* [rule-name]
|  |  +--rw rule-name                                 string
|  |  +--rw rule-description?                         string
|  |  +--rw rule-priority?                            uint8
|  |  +--rw enable?                                   boolean
|  |  +--rw session-aging-time?                       uint16
|  |  +--rw long-connection
|  |  |  +--rw enable?   boolean
|  |  |  +--rw during?   uint16
|  |  +--rw policy-event-clause-agg-ptr*              instance-identifier
|  |  +--rw policy-condition-clause-agg-ptr*          instance-identifier
|  |  +--rw policy-action-clause-agg-ptr*             instance-identifier
```

Modification of YANG module

- From a rule id to a rule name

OLD:

```
module: ietf-i2nsf-policy-rule-for-nsf
+--rw i2nsf-security-policy* [policy-name]
|  +--rw policy-name?            string
|  +--rw eca-policy-rules* [rule-id]
|  |  +--rw rule-id                                uint8
|  |  +--rw rule-description?                        string
|  |  +--rw rule-priority?                           uint8
|  |  +--rw policy-event-clause-agg-ptr*             instance-identifier
|  |  +--rw policy-condition-clause-agg-ptr*         instance-identifier
|  |  +--rw policy-action-clause-agg-ptr*            instance-identifier
```



NEW:

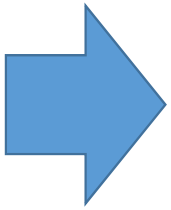
```
module: ietf-i2nsf-policy-rule-for-nsf
+--rw i2nsf-security-policy
|  +--rw policy-name?            string
|  +--rw rules* [rule-name]
|  |  +--rw rule-name                                 string
|  |  +--rw rule-description?                         string
|  |  +--rw rule-priority?                            uint8
|  |  +--rw enable?                                   boolean
|  |  +--rw session-aging-time?                       uint16
|  |  +--rw long-connection
|  |  |  +--rw enable?   boolean
|  |  |  +--rw during?   uint16
|  |  +--rw policy-event-clause-agg-ptr*              instance-identifier
|  |  +--rw policy-condition-clause-agg-ptr*          instance-identifier
|  |  +--rw policy-action-clause-agg-ptr*             instance-identifier
```

Modification of YANG module

- Default action

OLD:

```
|  +--rw default-action
|     +--rw default-action-type?   ingress-action
+--rw event-clause-container
|  ...
+--rw condition-clause-container
|  ...
+--rw action-clause-container
   ...
```



NEW:

```
+--rw default-action
|  +--rw default-action-type?   boolean
+--rw rule-group
   +--rw groups* [group-name]
      +--rw group-name     string
      +--rw rule-range
      |  +--rw start-rule?   string
      |  +--rw end-rule?     string
      +--rw enable?        boolean
      +--rw description?   string
-rw event-clause-container
 ...
-rw condition-clause-container
 ...
-rw action-clause-container
 ...
```

Addition of additional attributes for a policy

- Session time

```
module: ietf-i2nsf-policy-rule-for-nsf
+--rw i2nsf-security-policy
|  +--rw policy-name?                string
|  +--rw rules* [rule-name]
|  |  +--rw rule-name                                  string
|  |  +--rw rule-description?                          string
|  |  +--rw rule-priority?                             uint8
|  |  +--rw enable?                                    boolean
|  |  +--rw session-aging-time?                        uint16
|  |  +--rw long-connection
|  |  |  +--rw enable?   boolean
|  |  |  +--rw during?   uint16
|  |  +--rw policy-event-clause-agg-ptr*               instance-identifier
|  |  +--rw policy-condition-clause-agg-ptr*           instance-identifier
|  |  +--rw policy-action-clause-agg-ptr*              instance-identifier
```

Addition of additional attributes for a policy

- Rule group

```
+--rw default-action
|  +--rw default-action-type?   boolean
+--rw rule-group
   +--rw groups* [group-name]
      +--rw group-name      string
      +--rw rule-range
      |  +--rw start-rule?   string
      |  +--rw end-rule?     string
      +--rw enable?         boolean
      +--rw description?    string
-rw event-clause-container
 ...
-rw condition-clause-container
 ...
-rw action-clause-container
 ...
```

Addition of additional attributes for a policy

- Logs for a rule and a session

```
+--rw action-clause-container
   +--rw action-clause-list* [eca-object-id]
      +--rw entity-class?      identityref
      +--rw eca-object-id      string
      +--rw rule-log?          boolean
      +--rw session-log?       boolean
```

Addition of additional attributes for a policy

- Additional condition components

```
+--rw acl-number?                    uint32
+--rw application-condition
|  +--rw application-description?   string
|  +--rw application-object*        string
|  +--rw application-group*         string
|  +--rw application-label*         string
|  +--rw category
|     +--rw application-category* [name application-subcategory]
|        +--rw name                        string
|        +--rw application-subcategory    string
```

Application condition

```
+--rw url-category-condition
|  +--rw pre-defined-category*    string
|  +--rw user-defined-category*   string
```

URL category condition

Next Steps

- We will continue to work for the YANG data model of Object-Oriented (OO) Style.

- We will verify the YANG data model by implementing a prototype in the IETF Hackathon-103.
  - NSF-Facing Interface

I2NSF Registration Interface YANG Data Model

(draft-hyun-i2nsf-registration-interface-dm-05)

Sangwon Hyun, Jaehoon (Paul) Jeong,

Taekyun Roh, Sarang Wi and Jungsoo Park

Updates from the Previous Version

- The Previous Drafts:
  - draft-hyun-i2nsf-registration-interface-data-model-03
  - draft-hyun-i2nsf-registration-interface-data-model-04

- This draft defines a YANG Data Model (DM) corresponding to the Information Model (IM) for Registration Interface.
  - draft-hyun-i2nsf-registration-interface-im-06

- This YANG data module was verified through a prototype implemented at IETF-102 Hackathon.

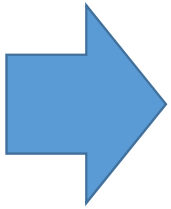
List of Changes

- Addition of a function for updating NSF capabilities
- Clarification and simplification of capabilities
- Addition of condition capabilities

Addition of a Function for Updating NSF Capabilities

OLD:

```
Instance Management Request
  +--rw i2nsf-instance-mgnt-req
    +--rw req-level uint16
    +--rw req-id uint64
    +--rw (req-type)?
      +--rw (instanciation-request)
        +--rw nsf-capability-information
        |  uses i2nsf-nsf-capability-information
      +--rw (deinstanciation-request)
        +--rw nsf-access-info
        |  uses i2nsf-nsf-access-info
```



NEW:

```
Instance Management Request
  +--rw i2nsf-instance-mgnt-req
    +--rw req-level uint16
    +--rw req-id uint64
    +--rw (req-type)?
      +--rw (instanciation-request)
        +--rw in-nsf-capability-information
        |  uses i2nsf-nsf-capability-information
      +--rw (deinstanciation-request)
        +--rw de-nsf-access-info
        |  uses i2nsf-nsf-access-info
      +--rw (updating-request)
        +--rw update-nsf-capability-information
        |  uses i2nsf-nsf-capability-information
```

Next Steps

- **WG Adoption Call** at IETF 102

- We will continue to work for the YANG data model of Object-Oriented (OO) Style.

- We will verify the YANG data model by implementing a prototype in the IETF Hackathon-103.
  - Registration Interface

YANG Data Model for Monitoring I2NSF Network Security Functions (draft-hong-i2nsf-nsf-monitoring-data-model-04)

Dongjin Hong, Jaehoon (Paul) Jeong, Jinyong (Tim) Kim,

Susan Hares, Liang Xia, and Henk Birkholz

Updates from the Previous Version

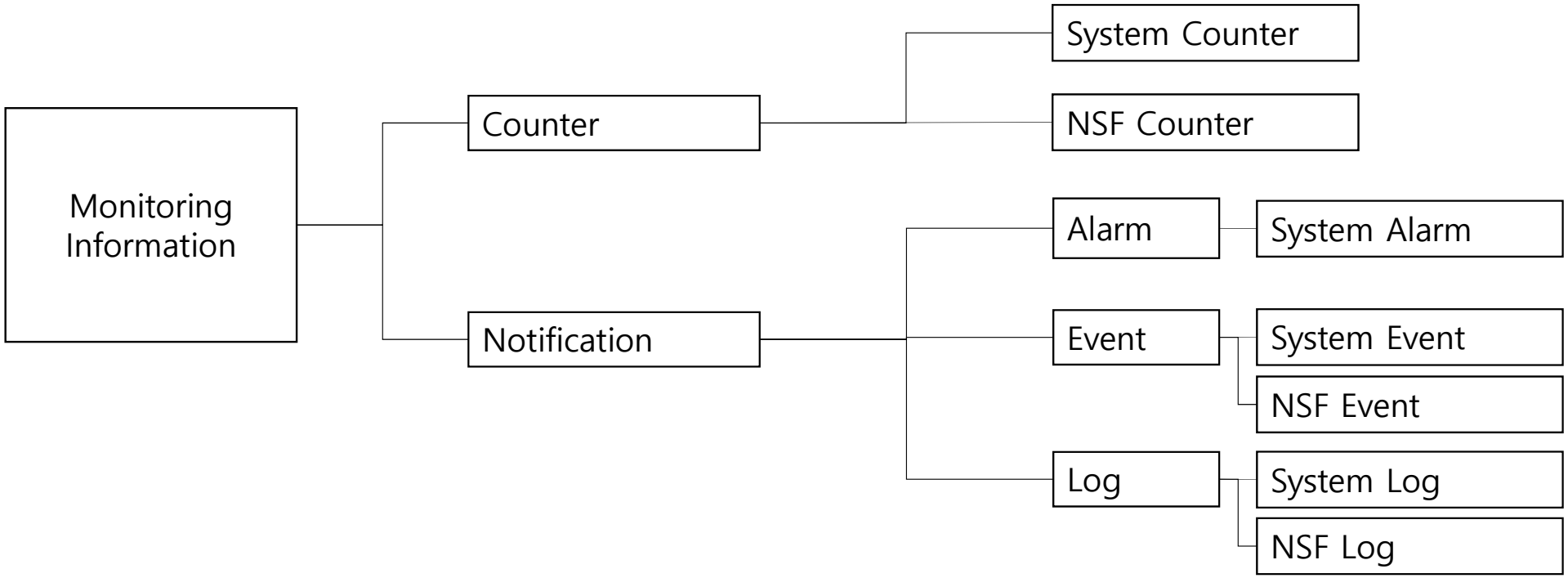
- The Previous Draft:
  - draft-hong-i2nsf-nsf-monitoring-data-model-03

- Changes from the previous versions
  - The YANG data model has been reorganized in detail by synchronizing with the latest information model:
    draft-zhang-i2nsf-info-model-monitoring-06

  - The YANG data model has been reorganized by a partial implementation based on ConfD.

Information and Data Models for NSF Monitoring

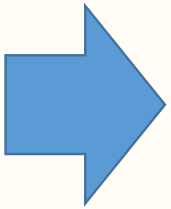
- The latest Information Model and YANG data model are synchronized as follows:



Addition of Monitoring Information Characteristics

OLD:

```
notifications:
  +---n system-detection-alarm
  |  +--ro alarm-catagory?    identityref
  |  +--ro usage?             uint8
  |  +--ro threshold?         uint8
  |  +--ro message            string
  |  +--ro time-stamp         yang:date-and-time
  |  +--ro severity           severity
```

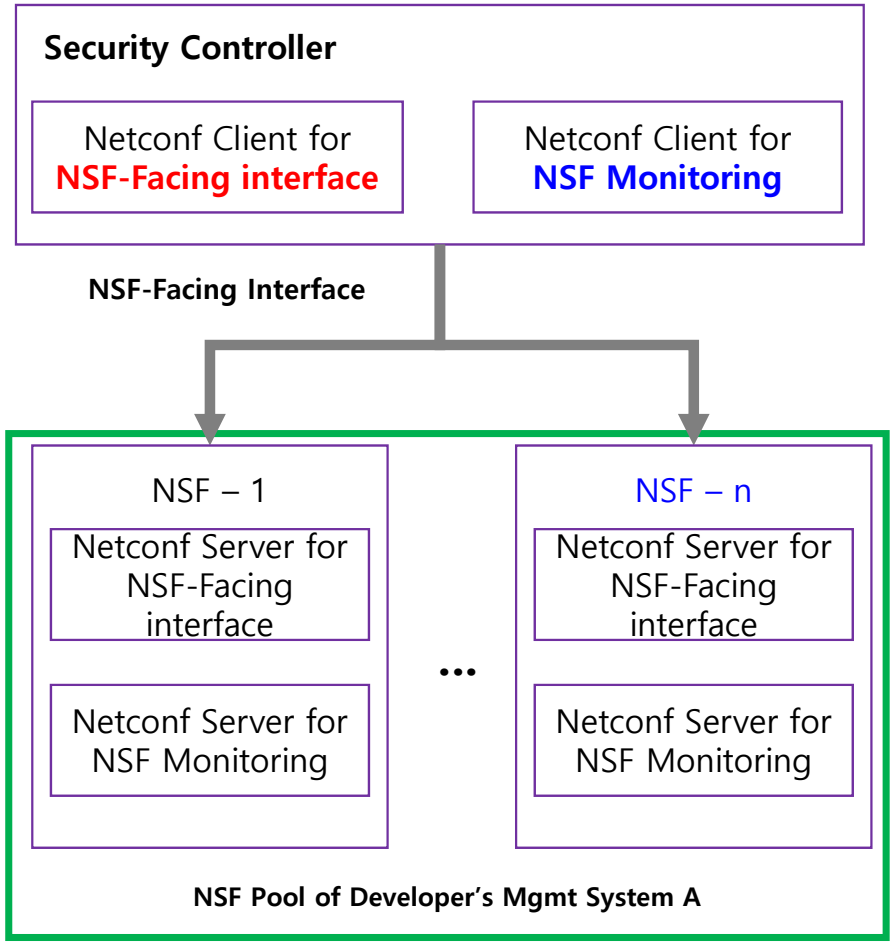


NEW:

```
notifications:
  +---n system-detection-alarm
  |  +--ro alarm-catagory?        identityref
  |  +--ro acquisition-method?    identityref
  |  +--ro emission-type?         identityref
  |  +--ro dampening-type?        identityref
  |  +--ro usage?                 uint8
  |  +--ro threshold?             uint8
  |  +--ro message?               string
  |  +--ro time-stamp?            yang:date-and-time
  |  +--ro vendor-name?           string
  |  +--ro nsf-name?              string
  |  +--ro module-name?           string
  |  +--ro severity?              severity
```

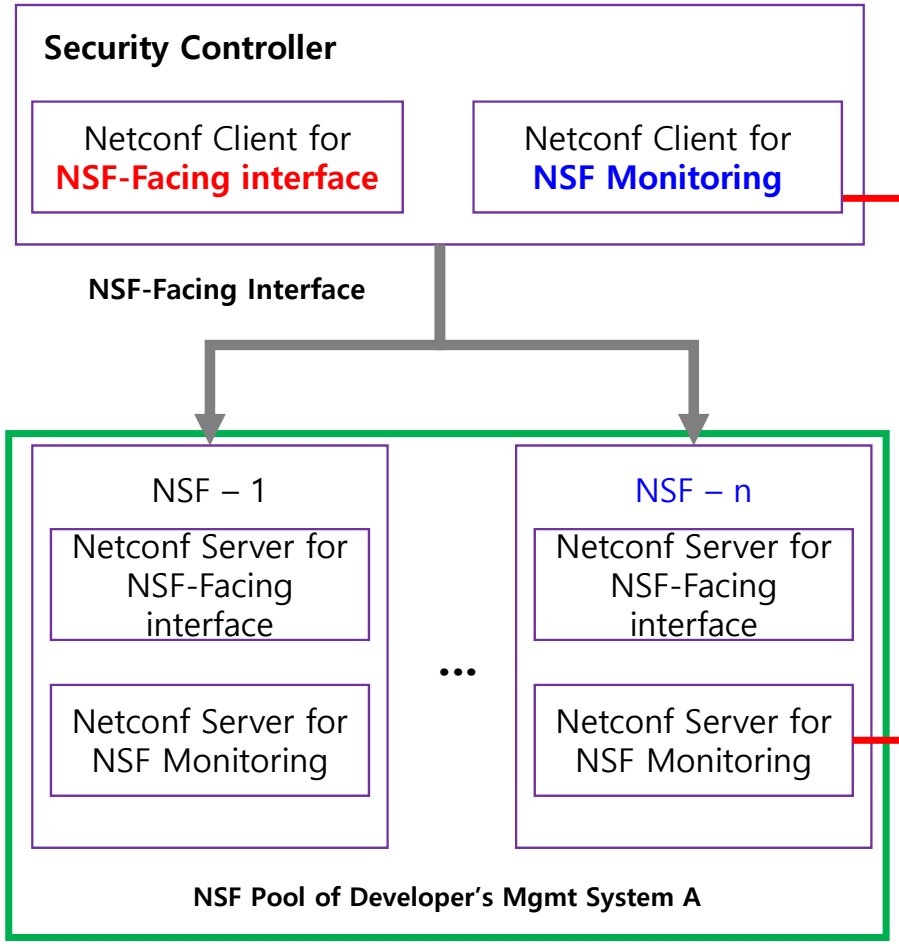
Implementation (1/2)

- Partial Implementation



Implementation (2/2)

- Partial Implementation




```
secu@secu:~/Hackathon/Hackathon-101/FullVersion/sc-basic$ sudo make subscribe
../../../../confd-6.2/bin/netconf-console-tcp -s all sub.xml
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
  <ok/>
</rpc-reply>
<?xml version="1.0" encoding="UTF-8"?>
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2018-06-07T13:01:39.41885+00:00</eventTime>
  <system-log-res-util-report xmlns="http://tail-f.com/ns/test/monitor">
    <nsfId>1</nsfId>
    <nsfName>firewall</nsfName>
    <cpu-usage>1.3</cpu-usage>
    <memory-total>4029468</memory-total>
    <memory-use>1497684</memory-use>
    <in-traffic-rate>0</in-traffic-rate>
    <out-traffic-rate>0</out-traffic-rate>
  </system-log-res-util-report>
</notification>
```

```
LD_LIBRARY_PATH= ./notifier_builtin_replay_store -t
TRACE Connected (dp) to ConfD
TRACE Received daemon id 0
TRACE Connected (dp) to ConfD
TRACE Picked up old user session: 11 for user:system ctx:system
TRACE Picked up old user session: 10 for user:system ctx:system
TRACE Picked up old user session: 1 for user:system ctx:system
notifier started
sending resource report notification
TRACE NOTIFICATION_SEND interface
```

Next Steps

- **WG Adoption Call** at IETF 102

- Completion of Reorganization
  - We will reorganize the data model for the updated information model for NSF Monitoring.

- Configuration and Manipulation for Monitoring
  - Using NSF-Facing Interface

- Completion of Implementation
  - We will fully implement NSF Monitoring Data Model.
  - We will integrate Monitoring data model into NSF-Facing Interface.
  - We will verify our implementation at IETF-103 Hackathon.