Network Security Functions Facing Interface YANG Data Model
(draft-ietf-i2nsf-nsf-facing-interface-dm-00)

IETF 101, London
March 21, 2018

Jinyong (Tim) Kim [Presenter], Jaehoon Paul Jeong, Jung-Soo Park, Susan Hares, and Qiushi Lin
Updates from the Previous Version

• The Previous Draft:

• Now adopted as a new WG document:
  – 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-00.

• This YANG data module was verified through a prototype implemented at IETF-101 Hackathon.
List of Updates

• Modification of YANG Module Name
  – John’s Comments (Resolved)

• Modification of Time Zone
  – Dongyue’s Comments (Resolved)

• Addition of Port Number to Condition Clause
  – Dongyue’s Comments (Resolved)

• Modification of Choice-Case Structure into Container Structure
  – Dongyue’s Comments (Resolved)

• Consistency between Capability Information Model (IM) and NSF-Facing Interface YANG Data Model (DM)
  – John’s Comments (Ongoing)

• Object-Oriented Features
  – John’s Comments (Ongoing)
Modification of YANG Module Name

- The YANG module name becomes `ietf-i2nsf-policy-rule-for-nsf`.

**OLD:**

```yang
module: ietf-i2nsf-ngf-facing-interface
  +++rw generic-ngf
    +++rw i2nsf-security-policy* [policy-name]
      +++rw policy-name string
        +++rw time-zone
          +++rw start-time? yang:date-and-time
          +++rw end-time? yang:date-and-time
          +++rw eca-policy-rules* [rule-id]
            +++rw rule-id uint8
            +++rw rule-description? string
            +++rw rule-rev? uint8
            +++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
            +++rw resolution-strategy
              +++rw (resolution-strategy-type)?
                +++:-{fmr}
                +++:-{lmr}
                +++rw first-matching-rule? boolean
                +++rw last-matching-rule? boolean
                +++rw default-action
                  +++rw default-action-type? ingress-action
                  +++rw event-clause-container
                    +++rw condition-clause-container
                      +++rw action-clause-container
```

**NEW:**

```yang
module: ietf-i2nsf-policy-rule-for-nsf
  +++rw i2nsf-security-policy* [policy-name]
    +++rw policy-name string
      +++rw time-zone
          +++rw start-time? yang:date-and-time
          +++rw end-time? yang:date-and-time
          +++rw eca-policy-rules* [rule-id]
            +++rw rule-id uint8
            +++rw rule-description? string
            +++rw rule-rev? uint8
            +++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
            +++rw resolution-strategy
              +++rw (resolution-strategy-type)?
                +++:-{fmr}
                +++:-{lmr}
                +++rw first-matching-rule? boolean
                +++rw last-matching-rule? boolean
                +++rw default-action
                  +++rw default-action-type? ingress-action
                  +++rw event-clause-container
                    +++rw condition-clause-container
                      +++rw action-clause-container
```
Modification of Time Zone

- We added not only an absolute time zone but also a periodic time zone to eca-policy-rules.

OLD:

```yaml
module: ietf-12nsf-net-facing-interface
  +++rw generic-nsf
  | | +++rw time-zone
  | | | | +++rw start-time? yang:date-and-time
  | | | | +++rw end-time? yang:date-and-time
  | | +++rw eco-policy-rule* [rule-id]
  | | | | | +++rw policy-name string
  | | | | | | +++rw start-time? yang:date-and-time
  | | | | | | +++rw end-time? yang:date-and-time
```

NEW:

```yaml
module: ietf-12nsf-security-policy* [policy-name]
  | | +++rw policy-name string
  | | | | +++rw eco-policy-rule* [rule-id]
  | | | | | +++rw rule-id uint8
  | | | | | +++rw rule-description? string
  | | | | | +++rw rule-rev? uint8
  | | | | | +++rw rule-priority? uint8
  | | | | | +++rw policy-event-clause-agg-prt* instance-identifier
  | | | | | +++rw policy-condition-clause-agg-prt* instance-identifier
  | | | | | +++rw policy-action-clause-agg-prt* instance-identifier
  | | | | +++rw resolution-strategy
  | | | | | | +++rw (resolution-strategy-type)?
  | | | | | | | +++rw first-matching-rule? boolean
  | | | | | | | | +++rw day
  | | | | | | | | | | +++rw sunday? boolean
  | | | | | | | | | | +++rw monday? boolean
  | | | | | | | | | | +++rw tuesday? boolean
  | | | | | | | | | | +++rw wednesday? boolean
  | | | | | | | | | | +++rw thursday? boolean
  | | | | | | | | | | +++rw friday? boolean
  | | | | | | | | | | +++rw saturday? boolean
  | | | | | | | | | | +++rw month
  | | | | | | | | | | | | +++rw january? boolean
  | | | | | | | | | | | | +++rw february? boolean
  | | | | | | | | | | | | +++rw march? boolean
  | | | | | | | | | | | | +++rw april? boolean
  | | | | | | | | | | | | +++rw may? boolean
  | | | | | | | | | | | | +++rw june? boolean
  | | | | | | | | | | | | +++rw july? boolean
  | | | | | | | | | | | | +++rw august? boolean
  | | | | | | | | | | | | +++rw september? boolean
  | | | | | | | | | | | | +++rw october? boolean
  | | | | | | | | | | | | +++rw november? boolean
  | | | | | | | | | | | | +++rw december? boolean
```
Addition of Port Number to Condition Clause

- We added a port number to a condition clause.

OLD:

| --- rw packet-security-tcp-condition
| | +++ rw pkt-sec-cond-tcp-seq-num* uint32
| | +++ rw pkt-sec-cond-tcp-ack-num* uint32
| | +++ rw pkt-sec-cond-tcp-window-size* uint16
| | +++ rw pkt-sec-cond-tcp-flags* uint8
| | --- rw packet-security-udp-condition
| | +++ rw pkt-sec-cond-udp-length* string
| --- rw packet-security-icmp-condition
| | +++ rw pkt-sec-cond-icmp-type* uint8
| | +++ rw pkt-sec-cond-icmp-code* uint8
| | +++ rw pkt-sec-cond-icmp-seg-num* uint32

NEW:

| --- rw packet-security-tcp-condition
| | +++ rw pkt-sec-cond-tcp-src-port* inet:port-number
| | +++ rw pkt-sec-cond-tcp-dest-port* inet:port-number
| | +++ rw pkt-sec-cond-tcp-seq-num* uint32
| | +++ rw pkt-sec-cond-tcp-ack-num* uint32
| | +++ rw pkt-sec-cond-tcp-window-size* uint16
| | +++ rw pkt-sec-cond-tcp-flags* uint8
| | --- rw packet-security-udp-condition
| | +++ rw pkt-sec-cond-udp-src-port* inet:port-number
| | +++ rw pkt-sec-cond-udp-dest-port* inet:port-number
| | +++ rw pkt-sec-cond-udp-length* string
| --- rw packet-security-icmp-condition
| | +++ rw pkt-sec-cond-icmp-type* uint8
| | +++ rw pkt-sec-cond-icmp-code* uint8
| | +++ rw pkt-sec-cond-icmp-seg-num* uint32
Modification of Choice-Case Structure into Container Structure (1/2)

- We changed a choice-case structure into a container structure about a condition clause for a multiple configuration.

**OLD:**

```xml
+++rw condition-clause-container
    +++rw condition-clause-list* [eca-object-id]
        +++rw entity-class?
        +++rw eca-object-id
        +++rw [condition-type]?
            +++:(packet-security-condition)
                | ...
                +++:(packet-payload-condition)
                    | ...
                +++:(target-condition)
                    | ...
                +++:(users-condition)
                    | ...
                +++:(context-condition)
                    | ...
                +++:(gen-context-condition)
        ...
+++rw action-clause-container
    ...
```

**NEW:**

```xml
+++rw condition-clause-container
    +++rw condition-clause-list* [eca-object-id]
        +++rw entity-class?
        +++rw eca-object-id
        +++rw [condition-type]?
            +++rw packet-security-condition
                ...
            +++rw packet-payload-condition
                ...
            +++rw target-condition
                ...
            +++rw users-condition
                ...
            +++rw context-condition
                ...
            +++rw gen-context-condition
                ...
        ...
+++rw action-clause-container
    ...
```
Modification of Choice-Case Structure into Container Structure (2/2)

- We changed a choice-case structure into a container structure about an action clause for a multiple configuration.

OLD:

```
module: ietf-12nsf-nsf-facing-interface
  +-rw generic-nsf
      |  +-rw 12nsf-security-policy* [policy-name]
      |     ...                    
      |     +-rw eca-policy-rules* [rule-id]
      |     ...                    
      |     +-rw resolution-strategy
      |     ...                    
      |     +-rw default-action
      |     ...                    
      |     +-rw event-clause-container
      |     ...                    
      |     +-rw condition-clause-container
      |     ...                    
      |     +-rw action-clause-container
      |     +-rw action-clause-list*[eca-object-id]
      |        +-rw entity-class?
      |        +-rw eca-object-id
      |         +-rw (action-type)?
      |            |  +-:(ingress-action)
      |            |    ...                    
      |            |  +-:(egress-action)
      |            |    ...                    
      |            |  +-:(apply-profile)
      |            ...                    
```

NEW:

```
module: ietf-12nsf-policy-rule-for-nsf
  +-rw 12nsf-security-policy* [policy-name]
      |     ...                    
      |     +-rw eca-policy-rules* [rule-id]
      |     ...                    
      |     +-rw resolution-strategy
      |     ...                    
      |     +-rw default-action
      |     ...                    
      |     +-rw event-clause-container
      |     ...                    
      |     +-rw condition-clause-container
      |     ...                    
      |     +-rw action-clause-container
      |     +-rw action-clause-list*[eca-object-id]
      |        +-rw entity-class?
      |        +-rw eca-object-id
      |         +-rw ingress-action
      |         ...                    
      |         +-rw egress-action
      |         ...                    
      |         +-rw apply-profile
      |         ...                    
```
Consistency between Capability IM and NSF-Facing Interface DM (Ongoing)

- We have modified event, condition, and action clauses to be aggregated into a policy.
Next Steps

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

• We will verify the OO YANG data model by implementing a prototype in the next Hackathon.