

Network Security Functions Facing Interface YANG Data Model (draft-kim-i2nsf-nsf-facing-interface-data-model-04)

Jinyong Tim Kim (Presenter), Jaehoon Paul Jeong, Jung-Soo Park, Susan Hares, and
Qiushi Lin

Date: 11/14/2017

Data Models

- **Capability Data Model:** To register the capabilities of NSFs into Security Controller.
 - <https://tools.ietf.org/html/draft-hares-i2nsf-capability-data-model-05>
- **NSF-Facing Interface Data Model:** To configure the policies into an NSF dynamically.
 - <https://tools.ietf.org/html/draft-kim-i2nsf-nsf-facing-interface-data-model-04>

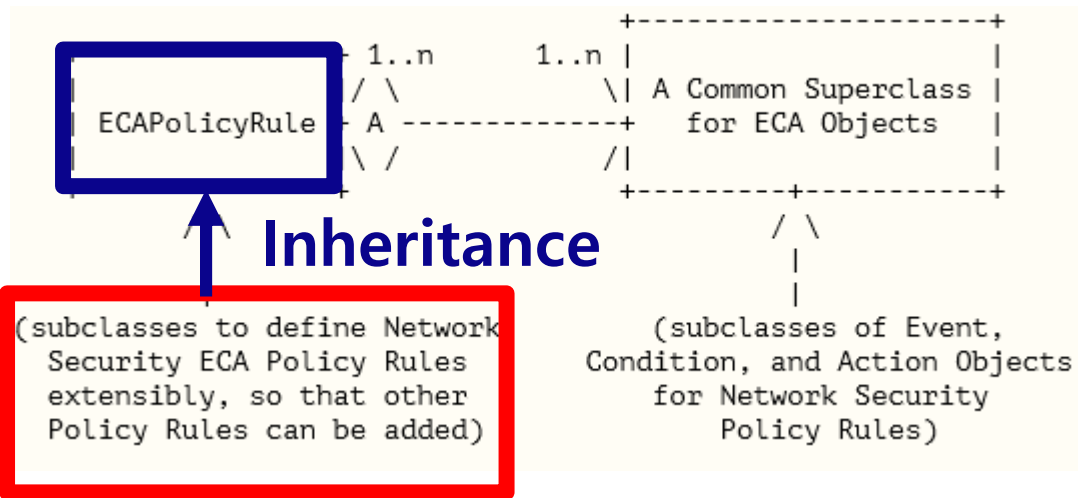
Introduction

- This draft is an updated version from **draft-kim-i2nsf-nsf-facing-interface-data-model-03**.
- This draft defines a YANG data model **corresponding to the information model for NSF-Facing Interface**.
 - **draft-ietf-i2nsf-capability-00**.
- This YANG data module **was verified through a prototype implemented at IETF-100 Hackathon**.

Major Changes of This Version

- **Capability Algebra**
 - Event/Condition/Action Clauses (**Resolved**)
 - Resolution Strategy Mechanism (**Resolved**)
 - Default Action Mechanism (**Resolved**)
- **Consistency** between Capability IM and NSF-Facing Interface Data Model
 - Object-Oriented Features (**Ongoing**)

Consistency between Capability IM and NSF-Facing Interface Data Model (1/6)

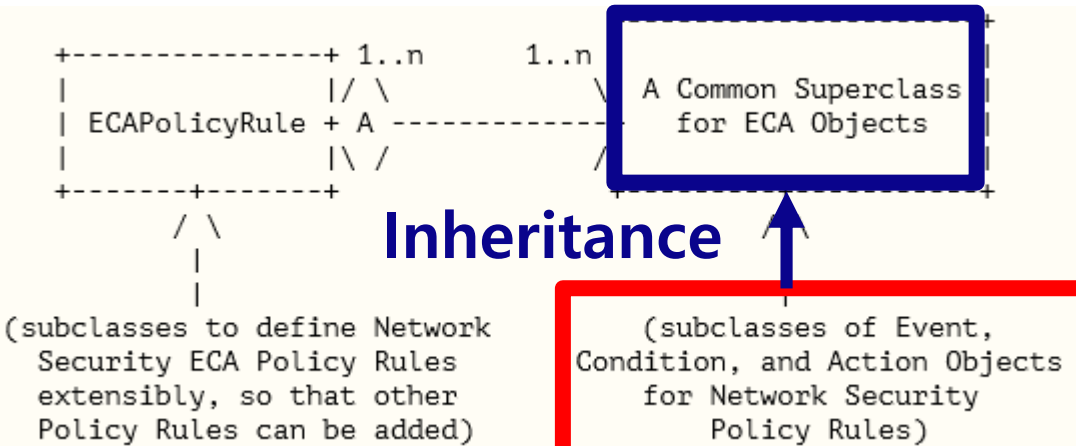


```

+--rw generic-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-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)?
|   |   |   |   +--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
|   ...
  
```

Mapping between IM and DM

Consistency between Capability IM and NSF-Facing Interface Data Model (2/6)



```

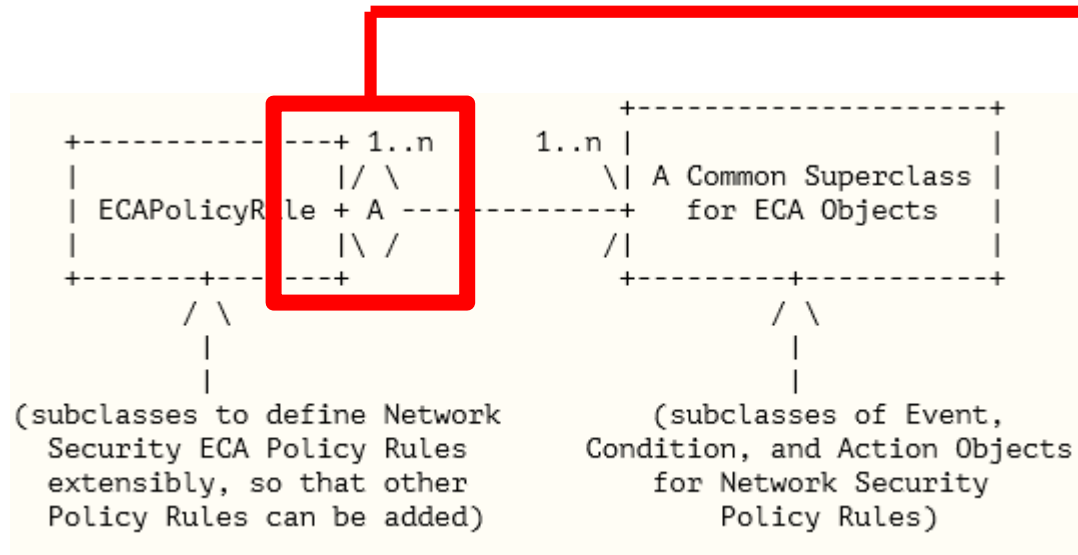
+--rw generic-nsf
|   +--rw i2nsf-security-policy* [policy-name]
|       +--rw policy-name          string
|       +--rw eca-policy-rules* [rule-id]
|           +--rw rule-id          uint8
|           +--rw rule-description? string
|           +--rw rule-rev?        uint8
|           +--rw rule-priority?   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
|   +--:( resolution-strategy-type)?
|       +--:( fmr)
|           +--rw first-matching-rule?  boolean
|       +--:( lmr)
|           +--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
|   ...

```

**Mapping
between IM and DM**

Consistency between Capability IM and NSF-Facing Interface Data Model (3/6)

Mapping between IM and DM

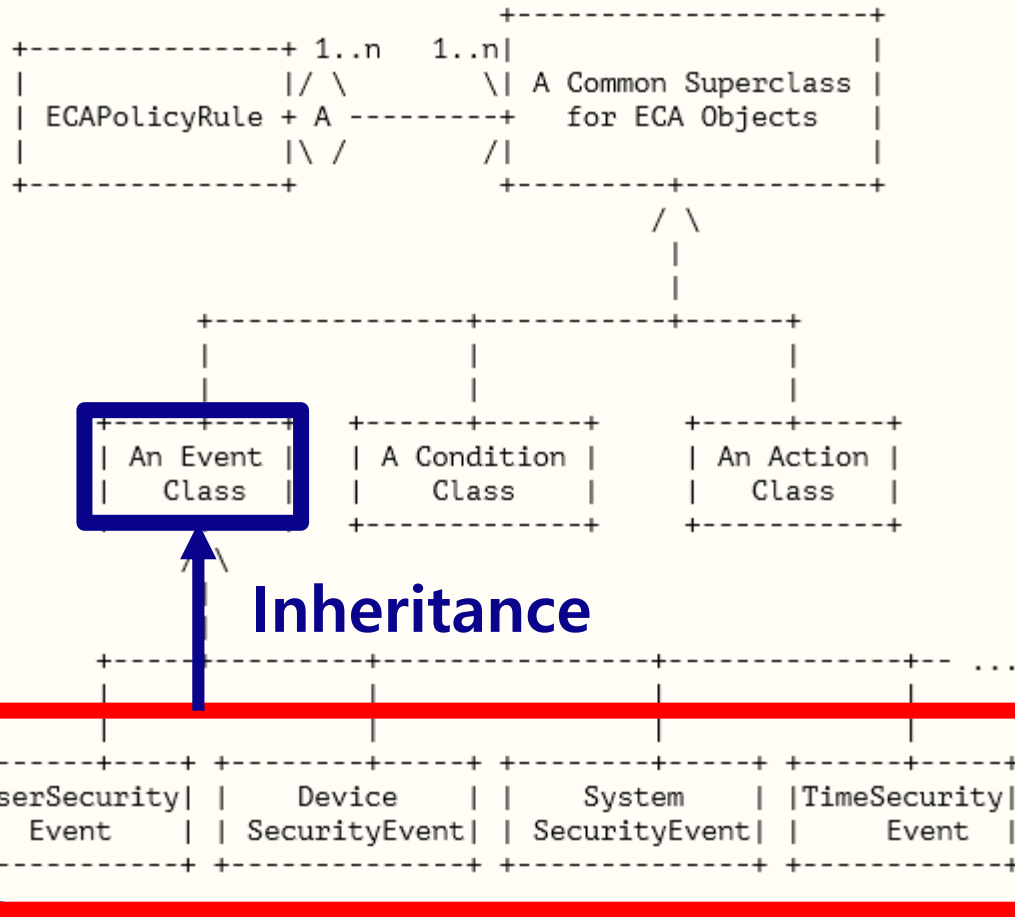


```

+--rw generic-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-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)
|           +--rw first-matching-rule? boolean
|       +--:(lmr)
|           +--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
|   ...
  
```

Aggregation Relation

Consistency between Capability IM and NSF-Facing Interface Data Model (4/6)



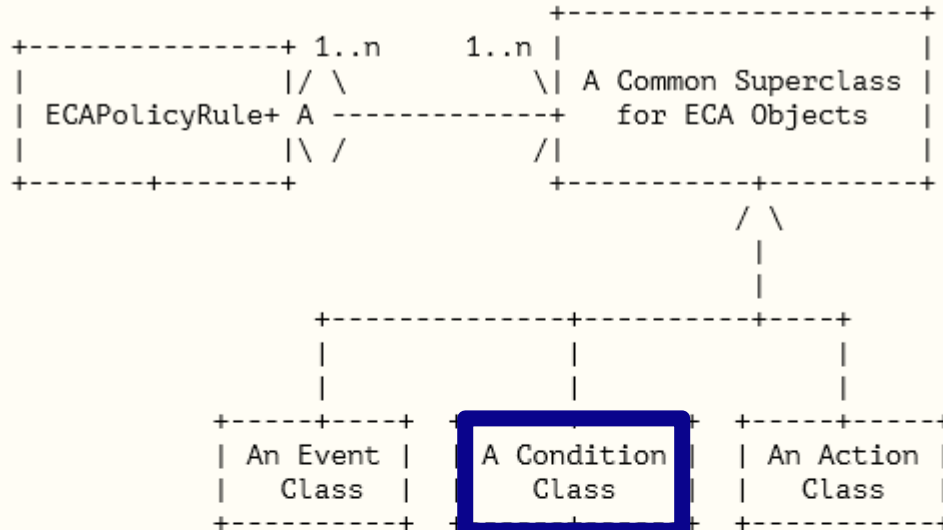
```

module: ietf-i2nsf-nsf-facing-interface
+--rw generic-nsf
|   +--rw i2nsf-security-policy* [policy-name]
|       ...
|       +--rw eca-policy-rules* [rule-id]
|           ...
|       +--rw resolution-strategy
|           ...
|       +--rw default-action
|           ...
+--rw event-clause-container
|   +--rw event-clause-list* [eca-object-id]
|       +--rw entity-class?          identityref
|       +--rw eca-object-id          string
|       +--rw manual?                string
|       +--rw sec-event-content      string
|       +--rw sec-event-format       sec-event-format
|       +--rw sec-event-type         string
+--rw condition-clause-container
|   ...
+--rw action-clause-container

```

Mapping between IM and DM

Consistency between Capability IM and NSF-Facing Interface Data Model (5/6)



Inheritance

```

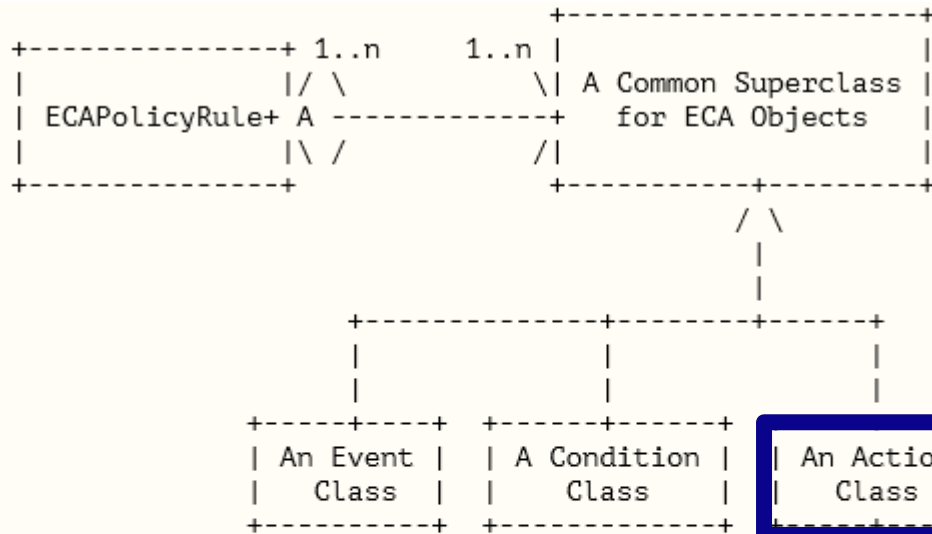
module: ietf-i2nsf-nsf-facing-interface
+--rw generic-nsf
|   +--rw i2nsf-security-policy* [policy-name]
|       ...
|       +--rw eca-policy-rules* [rule-id]
|           ...
|       +--rw resolution-strategy
|           ...
|       +--rw default-action
|           ...
+--rw event-clause-container
    
```

```

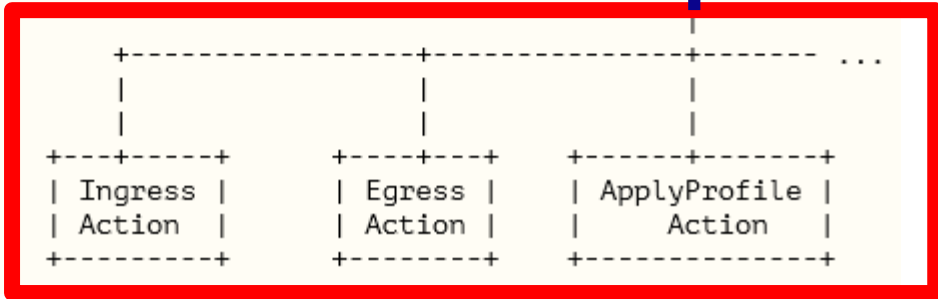
+--rw condition-clause-container
|   +--rw condition-clause-list* [eca-object-id]
|       +--rw entity-class?          identityref
|       +--rw eca-object-id          string
|       +--rw (condition-type)?
|           +--:(packet-security-condition)
|           |   ...
|           +--:(packet-payload-condition)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

Mapping between IM and DM

Consistency between Capability IM and NSF-Facing Interface Data Model (6/6)



Inheritance



```

module: ietf-i2nsf-nsf-facing-interface
+--rw generic-nsf
|   +--rw i2nsf-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?          identityref
|       +--rw eca-object-id          string
|       +--rw (action-type)?
|           +--:(ingress-action)
|               ...
|           +--:(egress-action)
|               ...
|           +--:(apply-profile)
|               ...
    
```

The code block shows YANG data model definitions. The 'action-clause-container' section is highlighted with a red box, showing a list of actions: 'ingress-action', 'egress-action', and 'apply-profile'.

Mapping between IM and DM

Next Steps

- 1. We will discuss with IM & DM team for consistency between IM and DM.
- 2. We will verify YANG data model by implementing a prototype.
- 3. We request WG Adoption.

Q&A

Thank you